635.17 Release of domestic incidents reports to the Army Family Advocacy Program (FAP).
635.18 Domestic violence.
635.19 Protection Orders.
635.20 Establishing Memoranda of Understanding.
635.21 Suspicious Activity Reporting (SAR).

Subpart D—Victim and Witness Assistance Procedures

635.22 Procedures.

Subpart E—National Crime Information Center Policy

635.23 Standards.

AUTHORITY: 28 U.S.C. 534, 42 U.S.C. 10601, 18 U.S.C. 922, 10 U.S.C. 1562, 10 U.S.C. Chap. 47, 42 U.S.C. 16901 *et seq.*, 10 U.S.C. 1565, 42 U.S.C. 14135a.

SOURCE: 80 FR 28549, May 19, 2015, unless otherwise noted.

Subpart A—Records Administration

§ 635.1 General.

The proponent of this part is the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to this Part that are consistent with controlling law and regulations. In distributing information on juvenile victims or subjects, the installation Freedom of Information Act (FOIA) Office will ensure that only individuals with a need to know of the personally identifiable information (PII) of a juvenile are provided the identifying information on the juvenile. For example, a community commander is authorized to receive pertinent information on juveniles under their jurisdiction. When a Law Enforcement Report identifying juvenile offenders must be provided to multiple commanders or supervisors, the FOIA Office must sanitize each report to withhold juvenile information not pertaining to that commander's area of responsibility.

[80 FR 28549, May 19, 2015, as amended at 81 FR 17386, Mar. 29, 2016]

§ 635.2 Safeguarding official information.

(a) Military police records are unclassified except when they contain national security information as defined in AR 380–5 (Available at *http://www.apd.army.mil/pdffiles/r380_5.pdf*), Department of the Army Information Security Program.

(b) Military police records will also be released to Federal, state, local or foreign law enforcement agencies as prescribed by 32 CFR part 505, The Army Privacy Program. Expanded markings will be applied to these records.

§ 635.3 Special requirements of the Privacy Act of 1974.

(a) Certain PII is protected in accordance with the provisions of the Privacy Act of 1974, 5 U.S.C. 552a, as implemented by 32 CFR part 310, DoD Privacy Program, 32 CFR part 505, The Army Privacy Program, and OMB guidance defining PII.

(b) Pursuant to 5 U.S.C. 552a(e)(3), when an Army activity asks an individual for his or her PII that will be maintained in a system of records, the activity must provide the individual with a Privacy Act Statement (PAS). A PAS notifies individuals of the authority, purpose, and use of the collection, whether the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.

(c) Army law enforcement personnel performing official duties often require an individual's PII, including SSN, for identification purposes. This PII can be used to complete law enforcement reports and records. In addition to Executive Order 9397, as amended by Executive Order 13478, the solicitation of the SSN is authorized by paragraph 2.c.(2) of DoD Instruction 1000.30, ''Reduction of Social Security Number (SSN) Use Within DoD'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/100030p.pdf*). The purpose is to provide commanders and law enforcement officials with means by which information may accurately be identified. The SSN is used as an additional/alternate means of identification to facilitate filing and retrieval. The following procedures will be used for identification:

(1) Retired military personnel are required to produce their Common Access Card or DD Form 2 (Ret) (U.S. Armed Forces of the United States

General Convention Identification Card), or other government issued identification, as appropriate.

(2) Family members of sponsors will be requested to produce their DD Form 1173 (Uniformed Services Identification and Privilege Card). Information contained thereon (for example, the sponsor's SSN) will be used to verify and complete applicable sections of law enforcement reports and related forms.

(3) Non-Department of Defense (DoD) civilians, including military family members and those whose status is unknown, will be advised of the provisions of the Privacy Act Statement when requested to disclose their PII, including SSN, as required.

(d) Notwithstanding the requirement to furnish an individual with a PAS when his or her PII will be maintained in a system of records, AR 340–21, The Army Privacy Program, *http://www.apd.army.mil/pdffiles/r340_21.pdf*, provides that records contained in SORN A0190–45, Military Police Reporting Program Records (MRRP), *http://dpcld.defense.gov/Privacy/SORNsIndex/tabid/5915/Article/6066/a0190-45-opmg.aspx*, that fall within 5 U.S.C. 552a(j)(2) are exempt from the requirement in 5 U.S.C. 552a(e)(3) to provide a PAS.

[80 FR 28549, May 19, 2015, as amended at 81 FR 17386, Mar. 29, 2016]

§ 635.4 Police intelligence/Criminal information.

(a) The purpose of gathering police intelligence is to identify individuals or groups of individuals in an effort to anticipate, prevent, or monitor possible criminal activity. Police intelligence aids criminal investigators in developing and investigating criminal cases. 32 CFR part 633 designates the U.S. Army Criminal Investigation Command (USACIDC) as having the primary responsibility to operate a criminal intelligence program. Criminal Intelligence will be reported through the Army Criminal Investigation and Criminal Intelligence (ACI2) System and other criminal intelligence products. The crimes listed in paragraphs (a)(1)–(9) of this section, as well as the reportable incidents, behavioral threat indicators, and other matters of counterintelligence interest specified by AR 381–12, Threat Awareness and Reporting Program, (available at *http://www.apd.army.mil/pdffiles/r381_12.pdf*) will be reported to the nearest Army counterintelligence office.

(1) Sedition;

(2) Aiding the enemy by providing intelligence to the enemy;

(3) Spying;

(4) Espionage;

(5) Subversion;

(6) Treason;

(7) International terrorist activities or material support to terrorism (MST);

(8) Unreported contacts with foreigners involved in intelligence activities;

(9) Unauthorized or intentional disclosure of classified info.

(b) Information on persons and organizations not affiliated with DoD may not normally be acquired, reported, processed or stored. Situations justifying acquisition of this information include, but are not limited to—

(1) Theft, destruction, or sabotage of weapons, ammunition, equipment facilities, or records belonging to DoD units or installations.

(2) Protection of Army installations and activities from potential threat.

(3) Information received from the FBI, state, local, or international law enforcement agencies which directly pertains to the law enforcement mission and activity of the installation Provost Marshal Office/Directorate of Emergency Services (PMO/DES), Army Command (ACOM), Army Service Component Command (ASCC) or Direct Reporting Unit (DRU) PMO/DES, or that has a clearly identifiable military purpose and connection. A determination that specific information may not be collected, retained or disseminated by intelligence activities does not indicate that the information is automatically eligible for collection, retention, or dissemination under the provisions of this part. The policies in this section are not intended and will not be used to circumvent any federal law that restricts gathering, retaining or dissemination of information on private individuals or organizations.

(c) Retention and disposition of information on non-DoD affiliated individuals and organizations are subject to the provisions of DoD Directive 5200.27